E-Commerce:-

What is Danial-of-service Attack?

A denial-of-service (DoS) attack is a concentrated, automated attempt to overload a target network with a large volume of requests to render it unavailable for use. It is achieved by launching a series of data packets very rapidly at a target computer system until it becomes too slow to be usable or is brought down entirely. The target system becomes slow as its central processing unit (CPU) attempts to handle the requests and serve responses. As the CPU grinds to a halt, any servers running on it — such as a web server powering your ecommerce store — become very latent or fully unresponsive altogether.

A DoS attack involves a single initiating source computer system. A distributed-denial-of-service (DDoS) attack is a much more serious version of DoS, however, and it involves reflecting and amplifying requests by enlisting hundreds or thousands of other source computers from across the globe to concentrate its efforts against the target.

Type of DoS Attacks:-

1. Volume (i.e. Network) based: This form of attack involves large numbers of requests being sent to the target system, and the system may perceive them to be valid requests (i.e. spoofed packets) or invalid requests (i.e. malformed packets). The goal of a volume based attack is to overwhelm your network capacity. The requests can be across a range of ports on your system. One type of method hackers use are UDP amplification attacks, whereby they send a request for data to a third party server spoofing your server’s IP address as the return address. The third party server then sends massive amounts of data to your server in response. In this way a hacker need only dispatch small requests himself, but your server will ultimately get lambasted with the “amplified” data from the third party servers. There could be tens, hundreds or thousands of systems involved in this form of attack.

2. Protocol based: Protocol based attacks are performed on load balancers or servers which exploit the way that systems communicate with each other. The packets can be designed to make the server wait for a non-existent response during

the normal handshake protocol, e.g. an SYN flood for example.

3. Application based: Hackers use known vulnerabilities in the web server software or application software to try to cause the web server to crash or hang. One common type of application based attack is to send partial requests to a server to attempt to use up (i.e. make busy) the entire database connection pool of the server which in turn blocks legitimate requests.

Preventative Measures:-

The first step in preparing for a potential attack is to setup a remote website monitoring service that will send out notifications when your online store becomes latent or goes down altogether. On the simple and cheap end, I use a service called BinaryCanary for many of our clients, but if you self-host with Amazon Web Services you can also set up hardware performance alarms via their CloudWatch service, which tracks various network I/O metrics and can also signal performance degradation, indicating that your store may be under a DoS or DDoS attack. Consider setting up an external logging service, as well. If your store comes under attack its web server logs may still be accessible from another source.

Another good practice is to point your DNS nameservers to a DDoS mitigation service such as CloudFlare. This can be useful later in making it harder for hackers to determine the actual location (i.e. IP addresses) of your servers. It acts as a proxy in front of your real systems and can be very useful as a front line of defense for large scale attacks that frankly most SMBs are utterly ill equipped to combat.

How to Mitigate the Attack:-

DDoS attacks are sophisticated and often involve vulnerabilities in low-level operating system or web server application software. WordPress (WP) for example had a recent XML-RPC reflection vulnerability that made it easy for hackers attempting a DDoS against a WordPress site or WP backed store. They can be very hard to mitigate without specialized knowledge. If you self host your own on-premise web server, you’re going to have to call in a third party that specializes in DDoS to help. Incapsula is one such providerTo mitigate an attack, you can either attempt to; absorb the attack or block the attack.

Absorbing the Attack

This may involve spinning up new servers, or provisioning new computers and a load balancer. This can quickly become very expensive, assuming your hosting environment is in the cloud to begin with. Provisioning an n-tier on-premise architecture, deploying more physical web servers, configuring and optimizing the application stack, adding a load balancer, etc. are all equipment used to bring high traffic websites to scale. Attempting to do this to absorb the attack (and organizations often attempt this, I've attempted it myself as well) to mitigate a DDoS is not only extremely time consuming and technically involved but it's also often a futile effort, as the DDoS amplifies it vastly outscales your ability to defend against it.

Blocking the Attack

This is a better approach than absorbing the attack, but here's where you'll need that third party service to profile the traffic so that you can effectively create a mitigation plan. You may get lucky and find a small number of IP addresses that are causing the problem. That would be the best case scenario, in which you could create firewall rules to block the address and be on your way. For a more serious internal DDoS mitigation environment if you're self hosting your own store, consider purchasing caching software and servers, picking up advanced hardware firewalls, a load balancer, etc. or other supporting network devices.